SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

EDWIN RAMIRO GALINDEZ VALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISTEMAS
POPAYAN - CAUCA 2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

EDWIN RAMIRO GALINDEZ VALENCIA

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMA

DIRECTOR:
Ing. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISTEMAS
POPAYÁN - CAUCA 2021

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

Popayán Cauca, 17 de noviembre de 2021

AGRADECIMIENTOS

En primer lugar, quiero agradecer a mi padre celestial quien ha sido un ser de luz y esperanza en mi vida, es quien ha forjado mi camino y me ha guiado para ir por el sendero correcto. En segunda instancia agradezco con toda mi alma a mis padres, quienes a pesar de las dificultades que se presentaron a lo largo de mi carrera, siempre me apoyaron y me motivaron a seguir adelante y a jamás darme por vencido. Su apoyo fue incondicional y puedo decir con toda seguridad que sin ellos no habría podido llegar a donde estoy hoy en día. En tercer lugar, agradezco también a mis dos hermanos, con los cuales crecimos juntos, bajo el mismo techo y con la cara sucia de tanto jugar, y aunque uno de ellos ya no está con nosotros, siempre lo llevare en lo más profundo de mi corazón. Por supuesto no podía faltar mi único hijo, que después de Dios soy yo quien más lo ama. Es el motor de mi vida, y por él decidí salir adelante y ser un profesional, a mi hijo gracias por ser mi principal motivación. Finalmente, quiero agradecer también a mis tutores, compañeros y por supuesto a la universidad, quienes en conjunto hicieron parte de este largo pero satisfactorio proceso de formación, y que me llevaron a convertirme en un profesional en lo que más me gusta y apasiona.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Enrutamiento: es un proceso como es el reenviar paquetes entre redes, claro está siempre buscando la mejor ruta o ruta más corta y que lleguen de forma adecuada. Es prácticamente un viaje que emprenden los paquetes los cuales en ese viaje atraviesan un sinnúmero de host o dispositivos de red intermedios. Debe existir algún mecanismo que sea capaz de direccionar los paquetes correctamente para que puedan alcanzar su destino final.

Host: también conocido como anfitrión, es una computadora o un dispositivo que está conectada a la red y su finalidad es proveernos un servicio. También sería una computadora donde esta guardada la información del servicio que necesitemos usar, como podría ser un servidor web o una base de datos y los usuarios se conectan a este servidor para interactuar con el servicio que este nos ofrece. Dicho en otras palabras, un host es un ordenador, el cual contiene datos o programas que otras computadoras van a poder acceder por medio de una red o modem.

Interfaces: se encargan de realizar una conexión física y lógica entre dos sistemas independientes, o bien entre un sistema informático y usuario-humano. Los sistemas pueden comunicarse mediante interfaces ya sean estándar de cable o inalámbricas.

Ping: comando que nos permite saber si llegamos a un determinado destino de forma correcta o, por el contrario, no podemos llegar a el. Sino recibimos una respuesta en un tiempo predeterminado, llegara un mensaje avisándonos de que no hay conexión con el host, ósea que la red es inalcanzable, por lo tanto, no se encuentra la ruta del host.

Router: es un dispositivo de hardware y se encarga de determinar las rutas por las que van a pasar los paquetes de datos, además va permitir que se interconecten ordenadores en la red. Los dispositivos que se encuentran conectados a internet en una vivienda, conforman una red de área local (LAN). Una vez que un módem recibe información de internet, el router la envía a los dispositivos personales.

Switch: si un router se encarga de la interconexión de las redes, los switches también se encargan de la interconexión de equipo, pero dentro de una misma red. También conocido como conmutador, es un dispositivo que sirve para conectar varios elementos dentro de una red. Dentro de una red local o LAN un Switch puede conectar varios dispositivos como una impresora, un PC, un televisor, una consola etc. Sencillamente el Switch se ocupa de emitir la información que recibe, para eso fue creado.

RESUMEN

En este primer escenario del programa Ingeniería de Sistemas de la UNAD, y donde se llevarán a cabo el desarrollo de las actividades correspondientes al Diplomado de Profundización CP CCNA1 y CCNA2 ll-2021 16-04 mediante la herramienta de Cisco Packet Tracer, donde se busca adquirir los conocimientos necesarios que nos lleven a configurar mediante la simulación de escenarios la correcta conectividad de los PCs dentro de las Redes LAN y WAN. También mediante la conmutación, nos va permitir que una señal llegue a su destino, después que esta salga de su origen. Finalmente, el enrutamiento que nos va a permitir determinar el mejor o el camino más óptimo de la ruta a la hora de reenviar paquetes entre redes.

En el segundo escenario, se va a configurar una red pequeña conformada por 3 Routers, 2 Switches, 2 PCs y un servidor de internet. Esta pequeña red admitirá conectividad IPc4 e IPv6. Para ingresar al modo CLI de los routers y switches se tendrá que realizar una validación de password, ya que estos cuenta con seguridad para acceder a ellos. Entre otros pasos, se inicializará y volverá a cargar los routers y switches, se configurará los parámetros básicos de los dispositivos, se configurará la seguridad del switch, las VLAN y el routing entre VLAN, se configurará el protocolo de routing dinámico OSPF, se implementará DHCP y NAT para IPv4, y finalmente se configurará y verificará las listas de control de acceso (ACL)

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this first scenario of the UNAD Systems Engineering program, and where the activities corresponding to the CP CCNA1 ll-2021 16-04 Diploma in Deepening will be carried out through the Cisco Packet Tracer tool, where it is sought to acquire the The necessary knowledge that leads us to configure the correct connectivity of the PCs within the LAN and WAN networks through the simulation of scenarios. Also by switching, it will allow a signal to reach its destination, after it leaves its origin. Finally, the routing that will allow us to determine the best or the most optimal path of the route when forwarding packets between networks.

In the second scenario, a small network made up of 3 routers, 2 switches, 2 PCs and an internet server will be configured. This small network will support both IPc4 and IPv6 connectivity. To enter the CLI mode of the routers and switches, a password validation will have to be performed, since they have security to access them. Among other steps, the routers and switches will be initialized and reloaded, the basic parameters of the devices will be configured, the switch security, VLANs and inter-VLAN routing will be configured, the OSPF dynamic routing protocol will be configured, it will be implemented DHCP and NAT for IPv4, and finally the access control lists (ACLs) will be configured and verified.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

El presente trabajo, va a permitir desarrollar las actividades propuestas para el Escenario 1. Escenario en el cual se van a configurar los dispositivos de una red pequeña, la cual será construida mediante el simulador. La red está compuesta por un Router, un Switch y dos PCs. Se diseñarán los respectivos esquemas de direccionamiento IPv4 para la LAN1 y la LAN2. Para el segundo escenario y al igual que la primera se va a configurar una pequeña red, la cual admitirá conectividad mediante IPv4 e IPv6, seguridad de routers y switches, entre otras configuraciones que contribuirán y darán las respectivas soluciones a los dos escenarios propuestos para este diplomado.

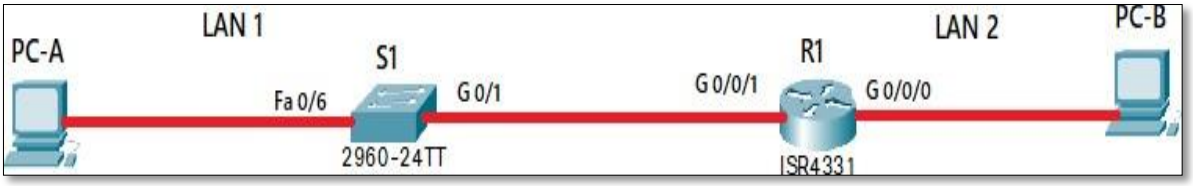
Mediante ajustes básicos de seguridad, se van a configurar el Router y el Switch, pues es de suma importancia que se de garantía a la seguridad de estos dispositivos. Entonces, se llevarán a cabo procesos como la creación de usuarios con sus respectivas contraseñas, para la habilitación del Router y Switch, y así poder ingresar al modo consola de estos y hacer las respectivas configuraciones de acuerdo a lo que se requiera.

Otro aspecto muy importante a tener en cuenta, es la configuración y la conectividad de los hosts. Ingresando al Command Prompt de cualquier host local contemplado dentro de la red de tipo TCP/IP y digitando el comando ping seguido de la dirección IP específica del host del cual deseamos recibir una respuesta en un tiempo predeterminado.

DESARROLLO

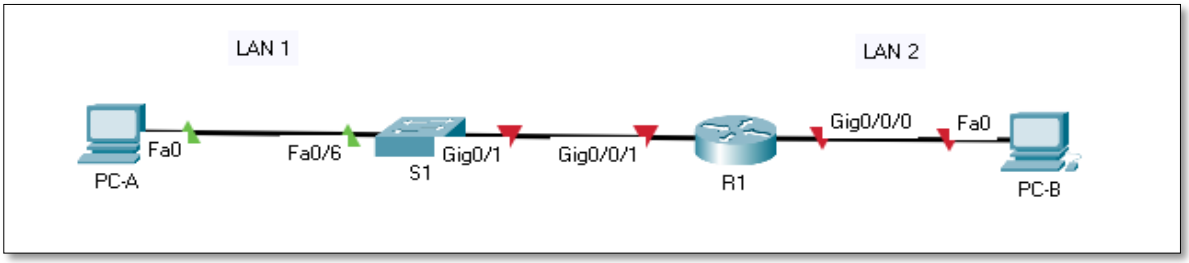
1. Escenario 1

Figura 1. Escenario propuesto



Fuente: Prueba de habilidades CISCO CCNA II

Figura 2. Simulación Escenario 1



Fuente: Elaboración propia

Parte 1: Construya la Red

En el simulador construya la red de acuerdo con la topología lógica que se plantea en la figura 1, cableeconforme se indica en la topología, y conecte los equipos de cómputo.

Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Cada estudiante tomara el direccionamiento 192.168.**X.**0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Direccionamiento

Item	Requerimiento
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula. 192.168.22.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.22.1/25
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.22.129/26
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.22.2
PC-A	Última dirección de host de la subred LAN1 192.168.22.126
PC-B	Última dirección de host de la subred LAN2 192.168.22.190

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre de dominio	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXECprivilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para lascontraseñas	R1(config)#security password min-length 10
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: admin Password: admin1pass R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd $ SOLO PERSONAL AUTORIZADO POR LA UNAD $
Configurar interfaz G0/0/0	R1(config)#interface g0/0/0 R1(config-if)#ip address 192.168.22.129 255.255.255.192 R1(config-if)#no shutdown R1(config-if)#exit
	R1(config)#interface g0/0/1

Configurar interfaz G0/0/1	R1(config-if)#ip address 192.168.22.1 255.255.255.128 R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 R1(config)# exit

1.1 Configuración del R1

1.1.1 Desactivar la búsqueda DNS

Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#no ip domain-lookup	Se desactiva la búsqueda DNS(R1)
R1#	

1.1.2 Nombre del Router

Router(config)#hostname R1 Asigno nombre al Router (R1)

1.1.3 Nombre del dominio

R1(config)#ip domain-name ccna-lab.com Se coloca nombre-dominio

1.1.4 Contraseña cifrada para el modo EXEC privilegiado

R1(config)#enable secret ciscoenpass

1.1.5 Contraseña de acceso a la consola

R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit

1.1.6 Establecer la longitud mínima para las contraseñas

R1(config)#security password min-length 10 Se configura la seguridad de la contraseña

1.1.7 Crear un usuario administrativo en la base de datos local

Nombre de usuario: **admin**
Password: **admin1pass**

R1(config)#username admin privilege 15 secret admin1pass

1.1.8 Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

R1(config)#line vty 04	Se configura line VTY 0 4
R1(config-line)#login local	Este paso, me va solicitar al contraseña al acceder
R1(config-line)#exit	Salimos

1.1.9 Configurar VTY solo aceptando las conexiones SSH

R1(config)#line vty 0 4

R1(config-line)#transport input ssh	Se activa únicamente la línea SSH en la línea de VTY
R1(config-line)#login local	
R1(config-line)#exit	Salimos

1.1.10 Cifrar las contraseñas de texto no cifrado

R1(config)#service password-encryption

1.1.11 Configurar un MOTD Banner

R1(config)#banner motd **$SOLO PERSONAL AUTORIZADO POR LA UNAD$**

1.1.12 Configurar Interfaz G0/0/0

R1#configure terminal	Ingreso a modo de configuración
R1(config)#interface g0/0/0	Configuro la interfaz
R1(config-if)#ip address 192.168.22.129 255.255.255.192	
R1(config-if)#no shutdown	Activo la interfaz
R1(config-if)#end	Finalizo

1.1.13 Configurar Interfaz G0/0/1

R1#configure terminal	Ingreso a modo de configuración
R1(config)#interface g0/0/1	Configuro la interfaz

R1(config-if)#ip address 192.168.22.1 255.255.255.128

R1(config-if)#no shutdown Activo la interfaz

R1(config-if)#end Finalizo

1.1.14 Generar una clave de cifrado RSA

R1(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024

R1(config)# exit

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd $ SOLO PERSONAL AUTORIZADO POR LA UNAD $ S1(config)#exit
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 S1(config)# exit
Configurar la interfaz de administración (SVI)	S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.22.2 255.255.255.128 S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#interface vlan 1 S1(config-if)#ip default-gateway 192.168.22.1 S1(config-if)#exit

1.2 Configuración del S1

1.2.1 Desactivar la búsqueda DNS

Switch>enable Ingreso a modo privilegiado
Switch#configure terminal Ingreso a modo de configuración
Switch(config)#no ip domain-lookup
Switch#

1.2.2 Nombre del Switch

Switch(config)#hostname S1 Asigno nombre al Switch (S1)
S1(config)#

1.2.3 Nombre de dominio

S1(config)#ip domain-name ccna-lab.com

1.2.4 Contraseña cifrada para el modo EXEC privilegiado

S1>enable secret ciscoenpass

1.2.5 Contraseña de acceso a la consola

```
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#
```

1.2.6 Crear un usuario administrativo en la base de datos local, con las siguientes credenciales:

Nombre de usuario: **admin**
Password: **admin1pass**

```
S1(config)#username admin privilege 15 secret admin1pass
```

1.2.7 Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#exit
S1(config)#
```

Se configura line VTY 0 15

1.2.8 Configurar las líneas VTY para que acepten únicamente las conexiones SSH

```
S1(config)#line vty 0 15
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
```

Se activa la línea SSH, en la línea de VTY

1.2.9 Cifrar las contraseñas de texto no cifrado

```
S1(config)#service password-encryption
```

1.2.10 Configurar un MOTD Banner

S1(config)#banner motd **$SOLO PERSONAL AUTORIZADO POR LA UNAD$**

1.2.11 Generar una clave de cifrao RSA

```
S1(config)#crypto key generate rsa
```

How many bits in the modulus [512]: 1024

S1(config)# exit

1.2.12 Configurar la interfaz de administración (SVI)

S1#configure terminal
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.22.3 255.255.255.128
S1(config-if)#no shutdown
S1(config-if)#end
S1(config-if)#wr

1.2.13 Configurar del Gateway predeterminado.

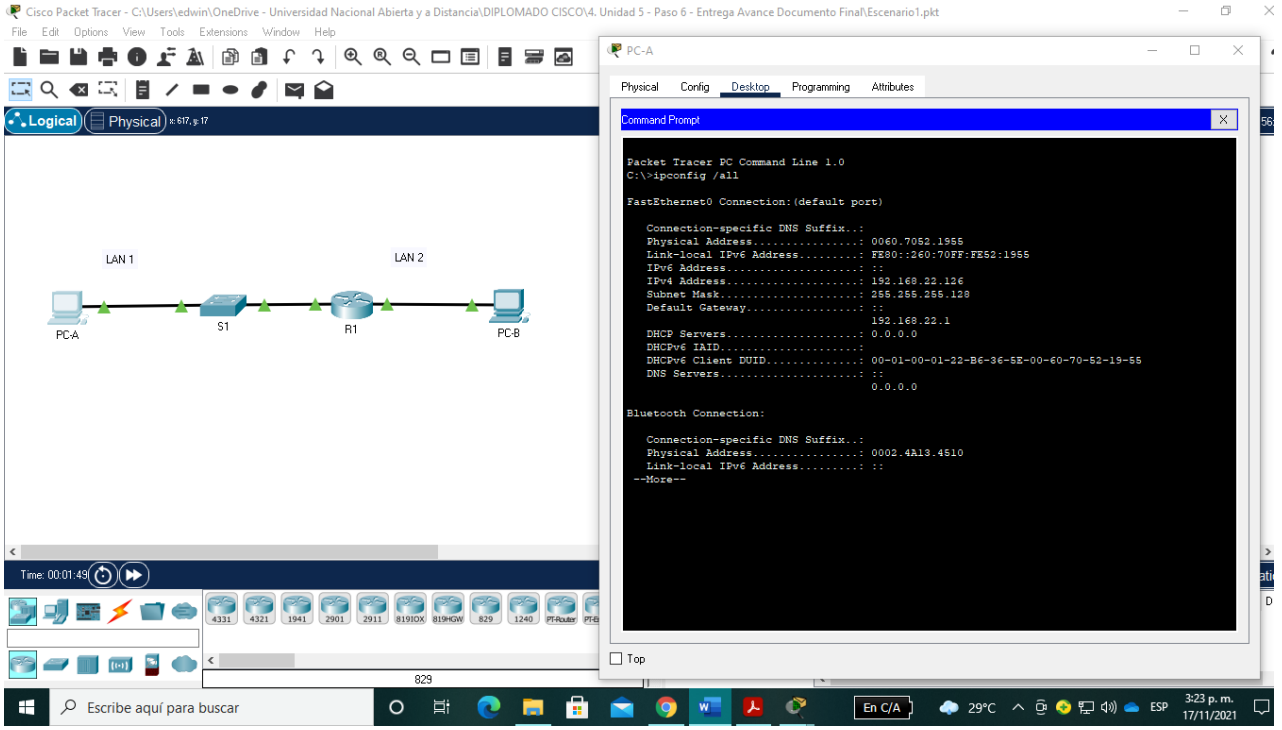
S1>enable
S1#configure terminal
S1(config)#interface vlan 1
S1(config-if)#ip default-gateway 192.168.22.1
S1(config-if)#end
S1(config-if)#wr

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre lasconfiguraciones de red del host con el comando **ipconfig /all**

Tabla 4. Configuración del PC-A

PC-A Network Configuration	
Descripción	
Dirección física	0060.7052.1955
Dirección IP	192.168.22.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.22.1

Figura 3. PC-A Network Configuration

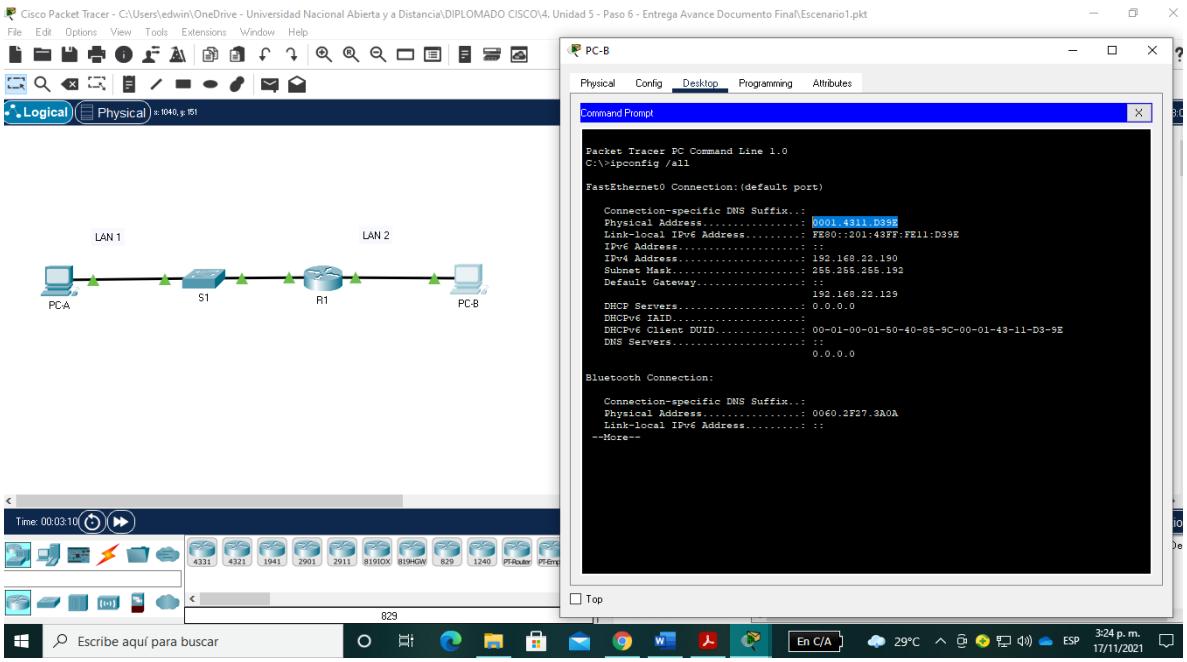


Fuente: Elaboración propia

Tabla 5. Configuración del PC-B

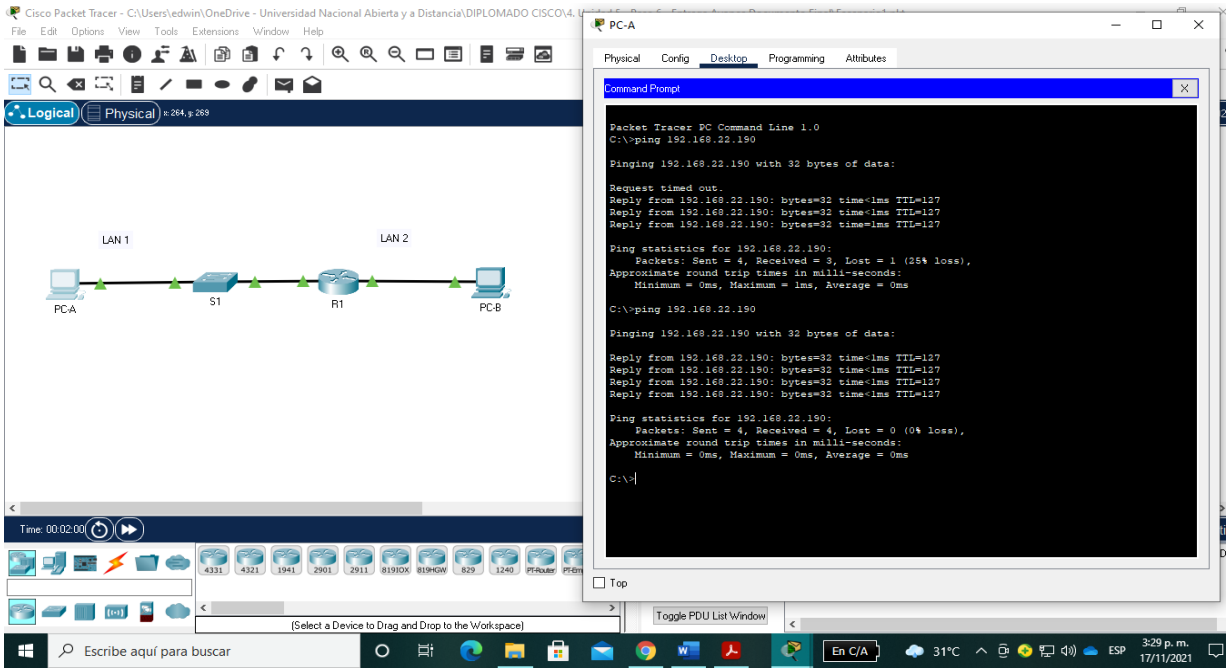
PC-B Network Configuration	
Descripción	
Dirección física	0001.4311.D39E
Dirección IP	192.168.22.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.22.129

Figura 4. PC-B Network Configuration



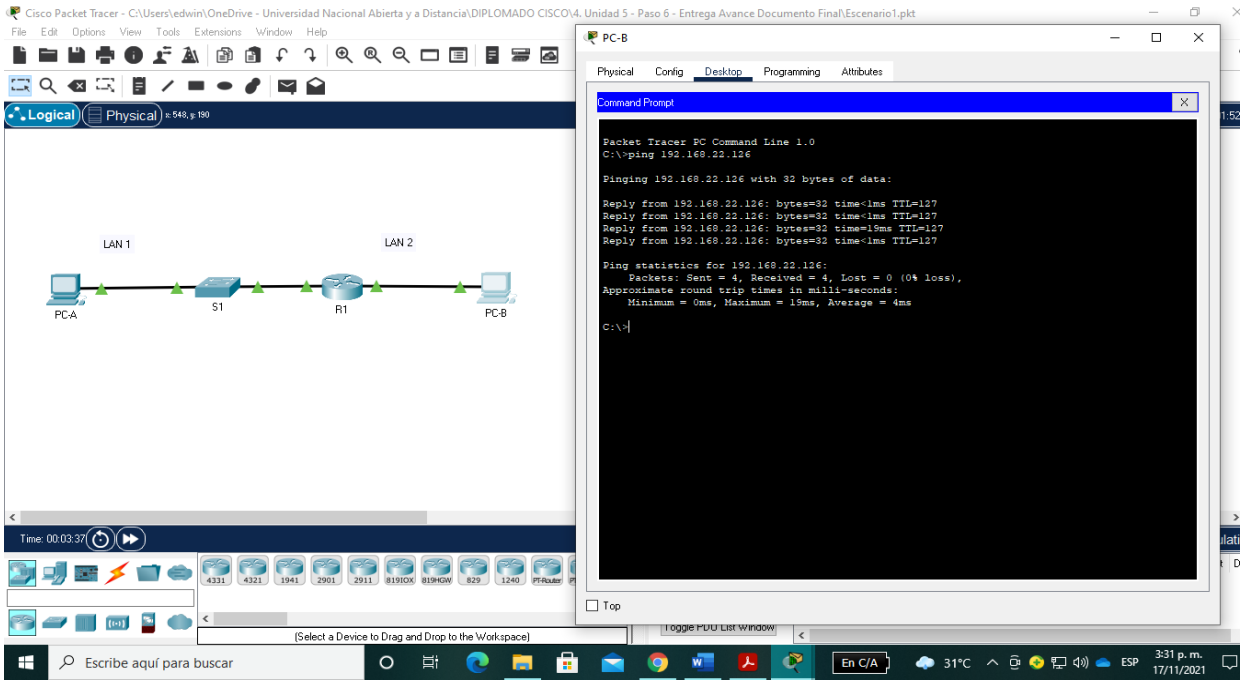
Fuente: Elaboración propia

Figura 5. Ping desde PC-A a PC-B



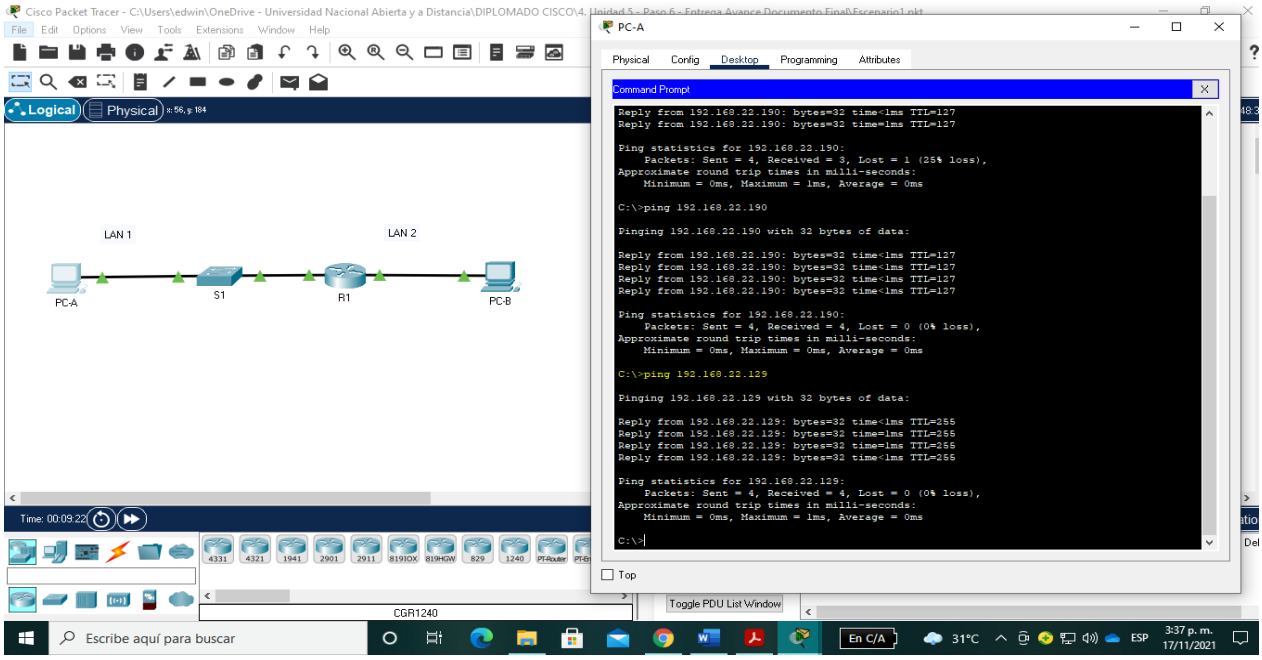
Fuente: Elaboración propia

Figura 6. Ping desde PC-B a PC-A



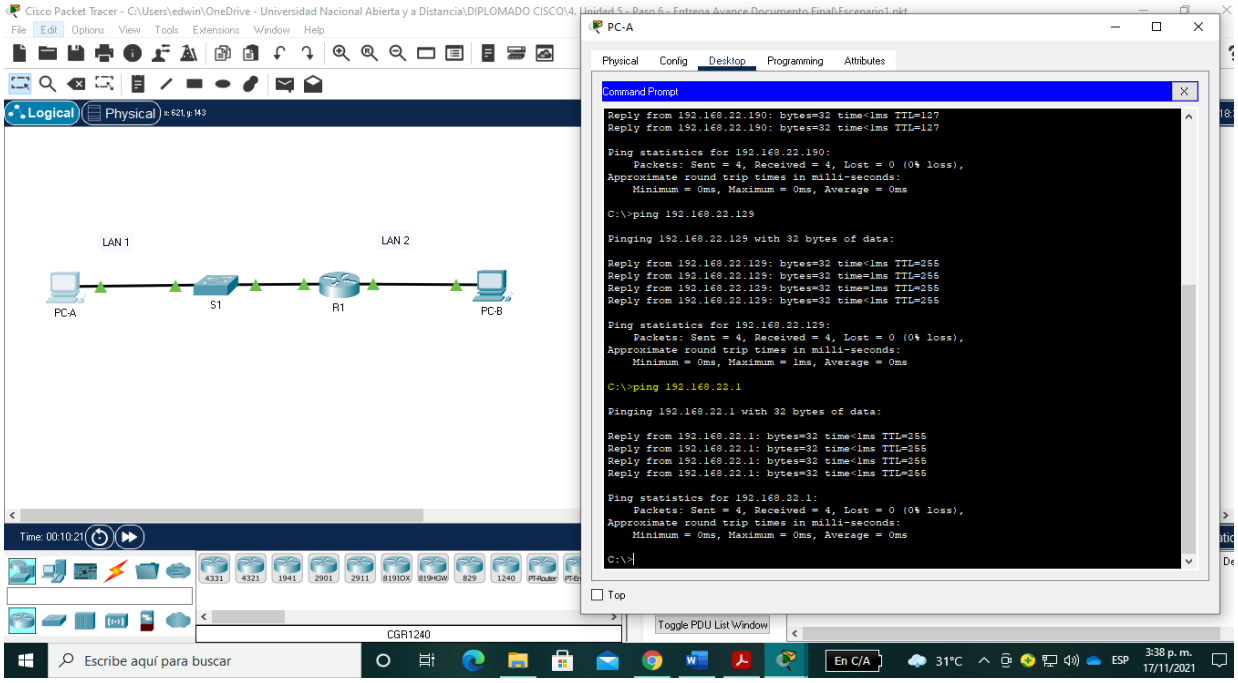
Fuente: Elaboración propia

Figura 7. Ping desde PC-A a R1 G0/0/0 192.168.22.129



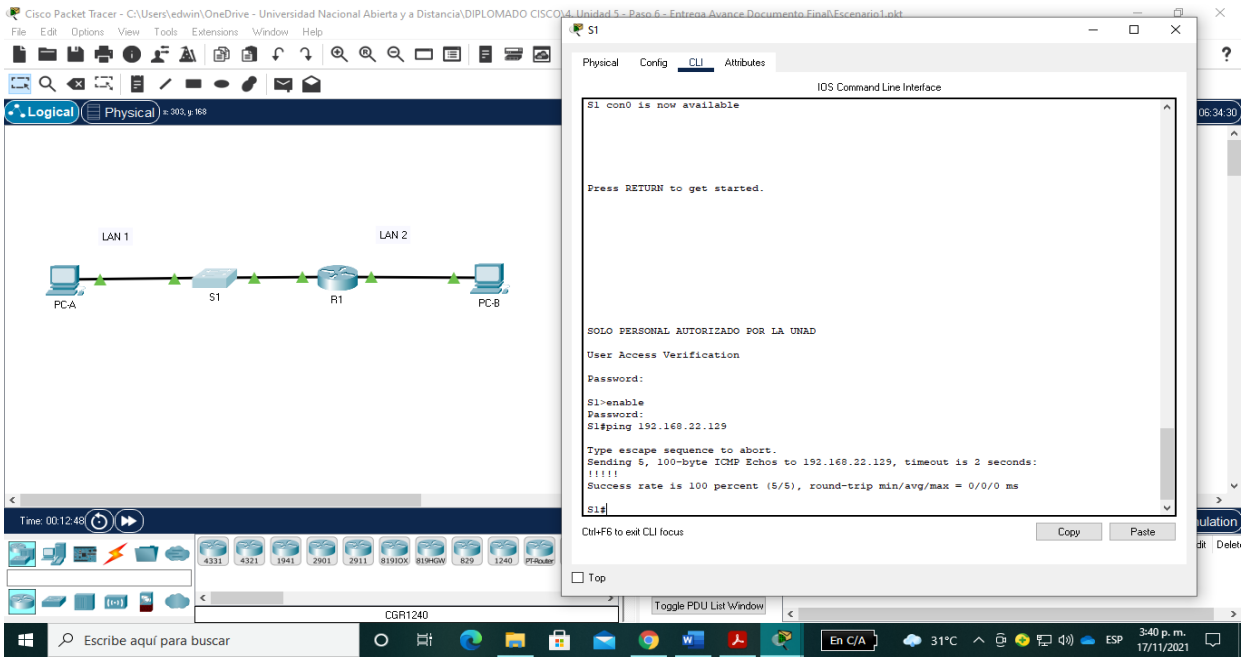
Fuente: Elaboración propia

Figura 8. Ping desde PC-A a R1 G0/0/1 192.168.22.1



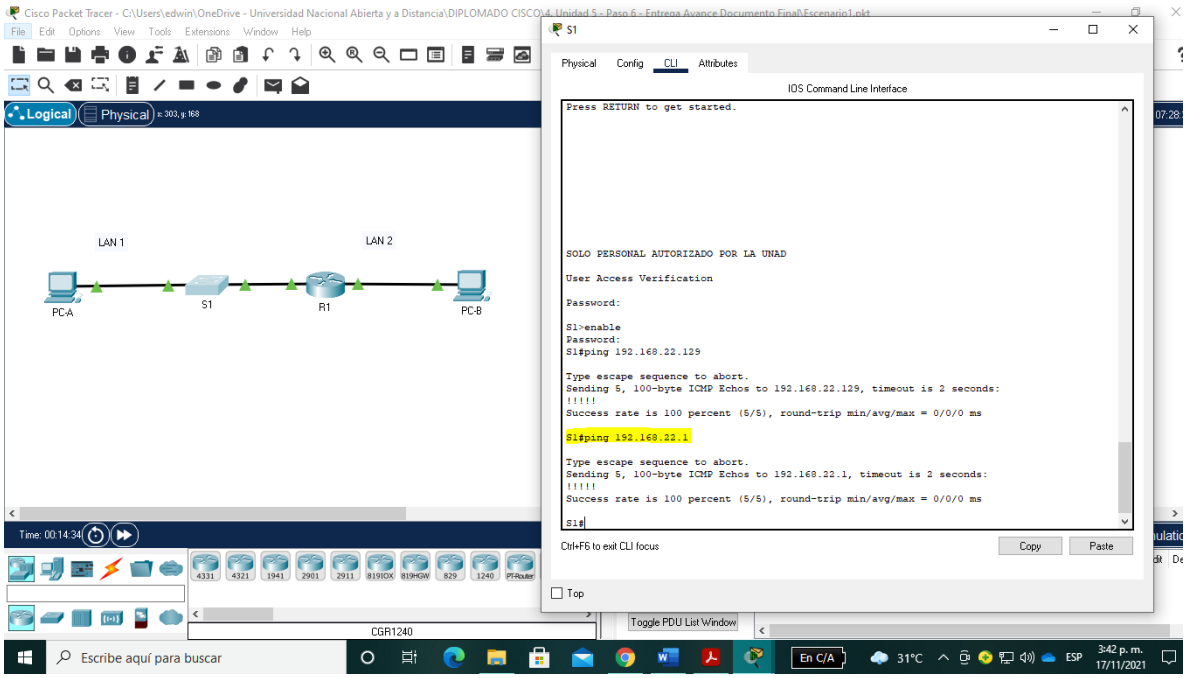
Fuente: Elaboración propia

Figura 9. Ping desde S1 a R1 G0/0/0 192.168.22.129



Fuente: Elaboración propia

Figura 10. Ping desde S1 a R1 G0/0/1 192.168.22.1

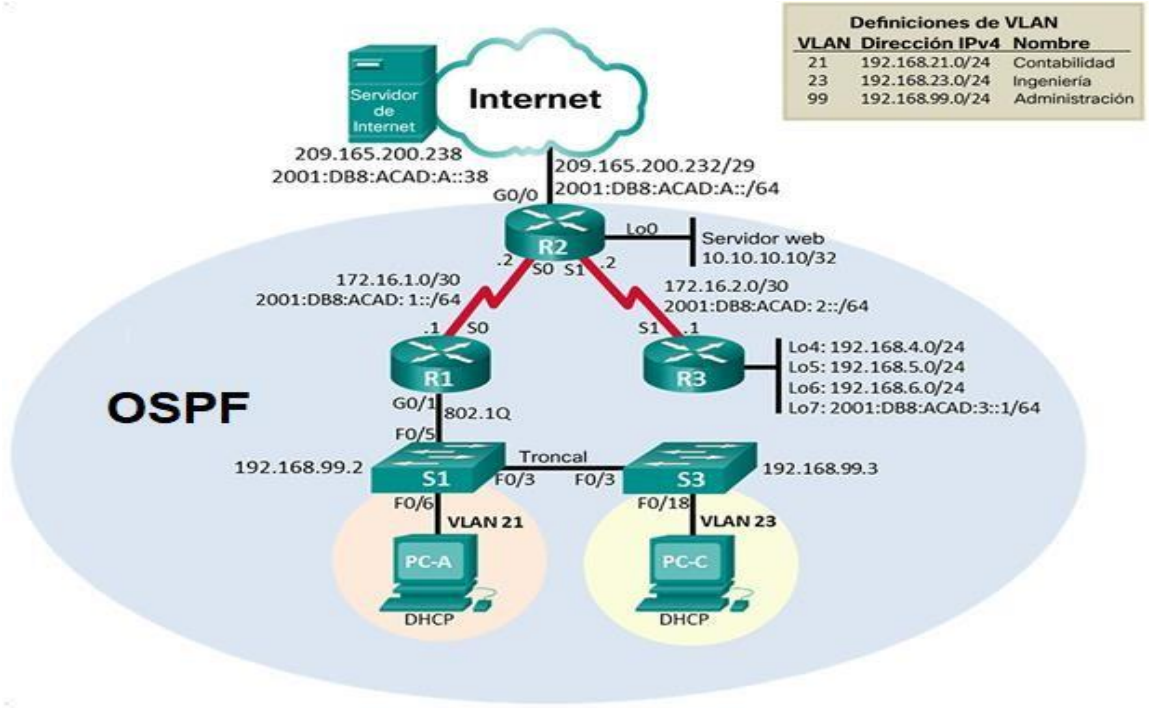


Fuente: Elaboración propia

2. Escenario 2

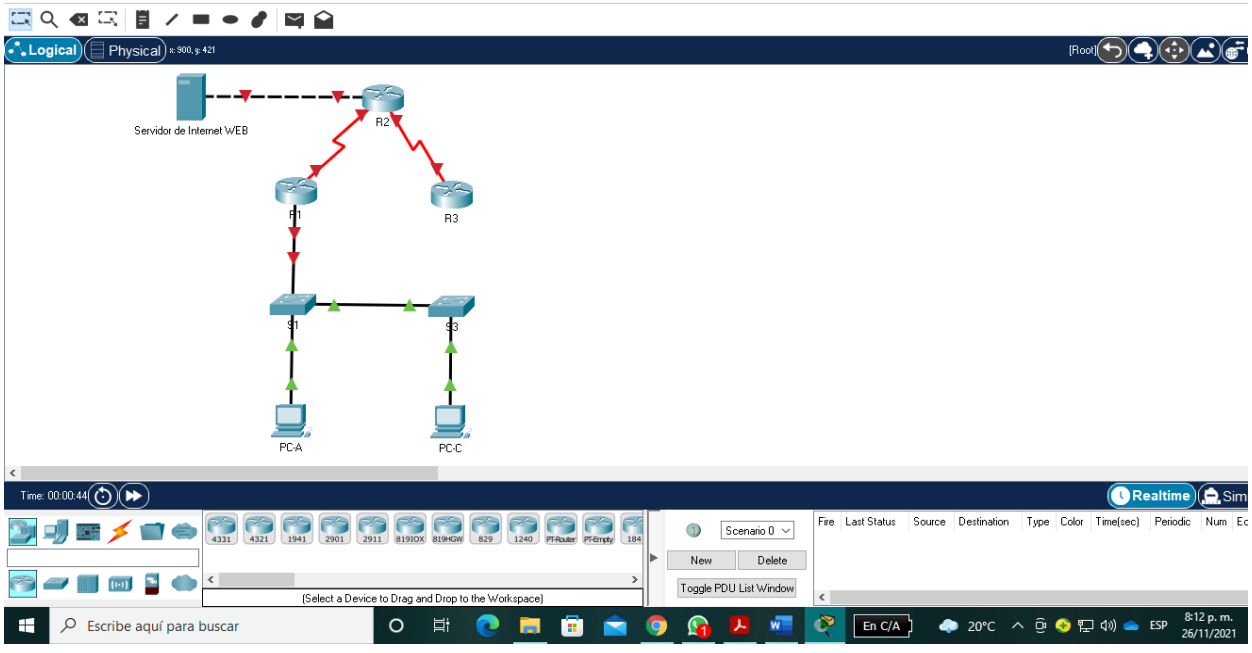
Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 11. Escenario propuesto



Fuente: Prueba de habilidades CCNA II

Figura 12. Simulación escenario 2.



Fuente: Elaboración propia

2.1 Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 6. Inicializar y volver a cargar los routers y los switches

Tarea	Comando IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config Erasing the nvram filesystem Will remove all configuration files! Continue [confirm] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Router>enable Router#reload Proceed with reolad? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase sta Switch#erase startup-config Erasing the nvram filesystem Will remove all configuration files! Continue [confirm] [OK] Erase of nvram: complete Switch#
Volver a cargar ambos switches	Switch>enable Switch#reload Proceed with reolad? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash: Directory of flash:/ 1 -rw- 4670455 <no date> c2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free) Switch#

2.2 Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 7. Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1(config)# enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)# password cisco R1(config-line)#login R1(config-line)# exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)# password cisco R1(config-line)#login R1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R1(config)# service password-encryption

Mensaje MOTD	R1(config)# banner motd $Se prohíbe el acceso no Autorizado$
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama detopología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz R1(config)# interface S0/0/0 R1(config)#description R1 a R2 R1(config-if)# ip address 172.16.1.1 255.255.255.252 R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)# clock rate 128000 R1(config-if)# no shutdown R1(config-if)# exit
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1 (config)# ip route 0.0.0.0 0.0.0.0 s0/0/0 R1 (config)# ipv6 route ::/0 s0/0/0 R1 (config)# ipv6 unicas R1 (config)#ipv6 unicast-routing R1 (config)#

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada	R2(config)# enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)# password cisco R2(config-line)#login R2(config-line)# exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)# password cisco R2(config-line)#login R2(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R2(config)# service password-encryption
Habilitar el servidor HTTP	Este comando no se puede ejecutar en ninguno de los routers de Packet Tracer
Mensaje MOTD	R2(config)# banner motd $Se prohíbe el acceso no autorizado$
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2(config)# interface S0/0/0 R2(config-if)# description R2 a R1 Router(config-if)# ip address 172.16.1.2 255.255.255.252 R2(config-if)# ipv6 address 2001:db8:acad:1::2/64 R2(config-if)# no shutdown R2(config-if)# exit

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz R2(config)# interface S0/0/1 R2(config-if)# description R2 a R3 R2(config-if)# ip address 172.16.2.2 255.255.255.252 R2(config-if)# ipv6 address 2001:db8:acad:2::2/64 R2(config-if)# clock rate 128000 R2(config-if)# no shutdown R2(config-if)# exit
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz R2(config)# interface G0/0 R2(config-if)# description R2 to Internet R2(config-if)# ip address 209.165.200.233 255.255.255.248 R2(config-if)# ipv6 address 2001:db8:acad:a::1/64 R2(config-if)# no shutdown R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config)# interface loopback 0 R2(config-if)# ip address 10.10.10.10

	255.255.255.255 R2(config-if)# exit
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Enter configuration commands, one per line. End with CNTL/Z Router(config)# no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)# enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)# password cisco R3(config-line)#login R3(config-line)# exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)# password cisco R3(config-line)#login R3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R3(config)# service password-encryption
Mensaje MOTD	R3(config)# banner motd $Se prohíbe el acceso no autorizado$
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

	Activar la interfaz R3(config)# interface S0/0/1 R3(config-if)# description R3 a R2 Router(config-if)# ip address 172.16.2.1 255.255.255.252 R3(config-if)# ipv6 address 2001:db8:acad:2::1/64 R3(config-if)# no shutdown R3(config-if)# exit
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 4 R3(config-if)# ip address 192.168.4.1 255.255.255.0 R2(config-if)# exit
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 5 R3(config-if)# ip address 192.168.5.1 255.255.255.0 R2(config-if)# exit
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)# interface loopback 6 R3(config-if)# ip address 192.168.6.1 255.255.255.0 R2(config-if)# exit
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)# interface loopback 7 R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)# exit R3(config-if)#ipv6 unicast-routing R3(config)#
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Enter configuration commands, one per line. End with CNTL/Z Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Contraseña de exec privilegiado cifrada	S1(config)# enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)# password cisco S1(config-line)#login S1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S1(config)# service password-encryption
Mensaje MOTD	S1(config)# banner motd $Se prohibe el acceso no autorizado$

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12. Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Enter configuration commands, one per line. End with CNTL/Z Switch(config)# no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	S3(config)# enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0

	S3(config-line)# password cisco S3(config-line)#login S3(config-line)# exit
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)# password cisco S3(config-line)#login S3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	S3(config)# service password-encryption
Mensaje MOTD	S3(config)# banner motd $Se prohibe el acceso no autorizado$

Paso 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

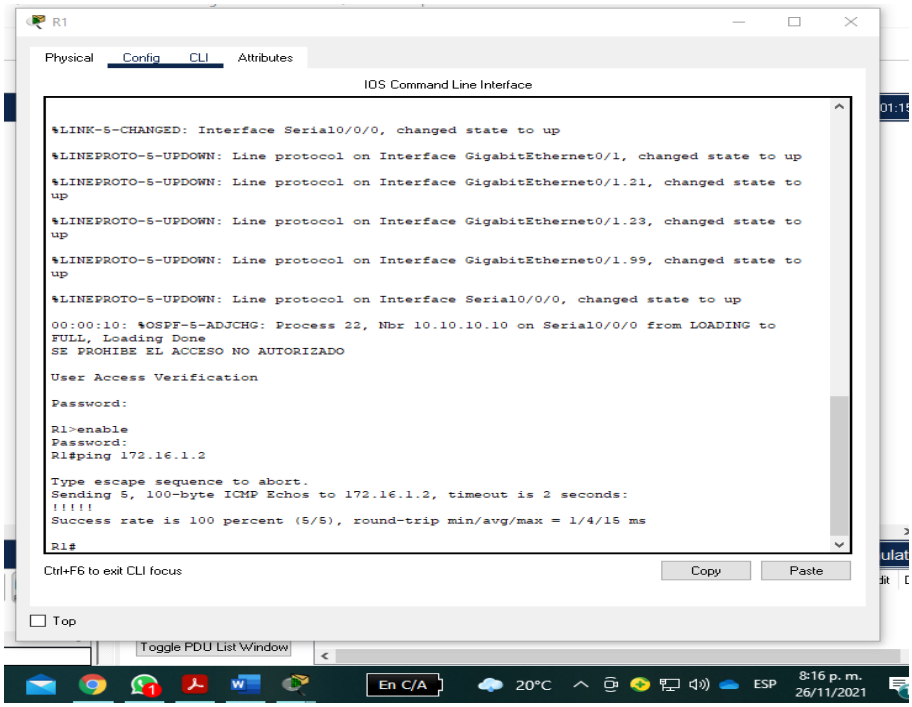
Tabla 13. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 12/16/25 ms
R2	R3, S0/0/1	172.16.2.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to

			172.16.2.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/24 ms
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time=1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Reply from 209.165.200.233: bytes=32 time<1ms TTL=255 Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

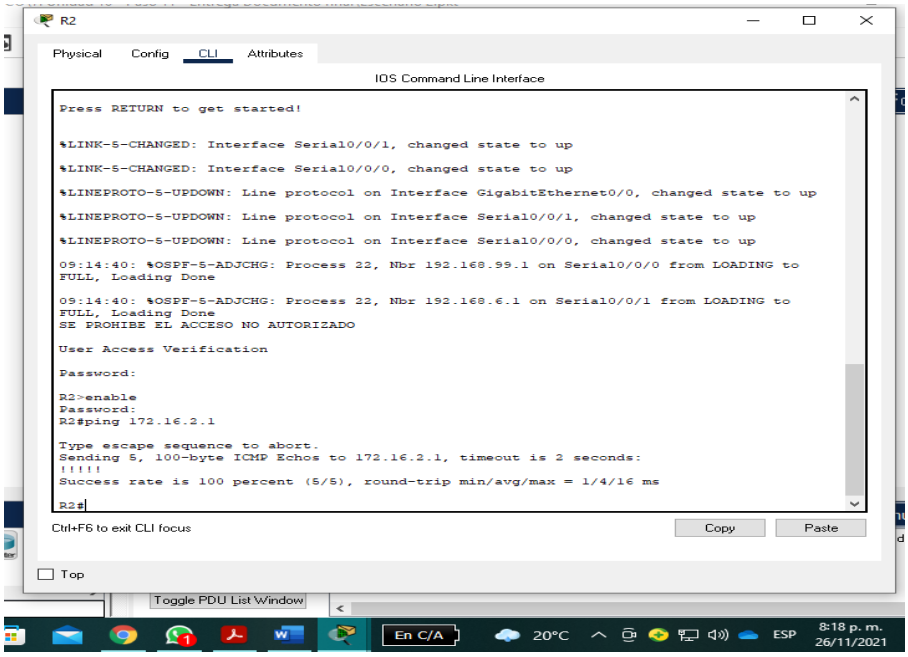
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicencorrectamente.

Figura 13. Ping de R1 a R2 S0/0/0



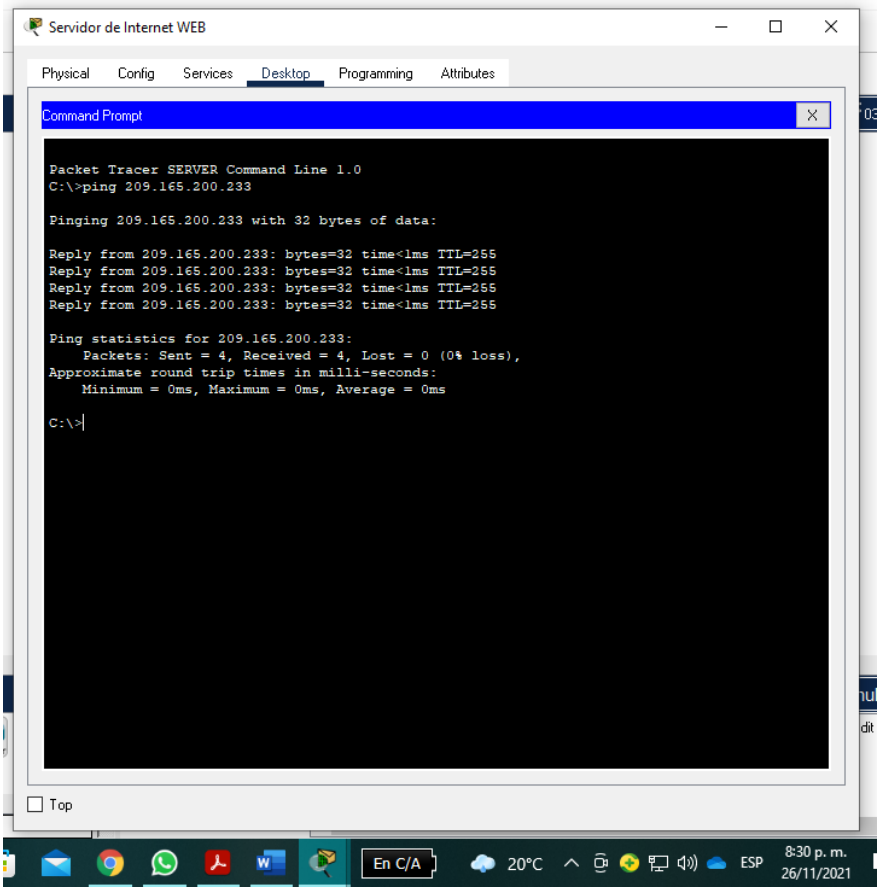
Fuente: Elaboración propia

Figura 14. Ping de R2 a R3 S0/0/1



Fuente: Elaboración propia

Figura 15. Ping PC Internet a Gateway predeterminado



Fuente: Elaboración propia

2.3 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14. Configuración de la seguridad S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican

	S1#config t S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)# name Administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama detopología S1(config)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config)#exit
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como elgateway predeterminado. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface f0/3 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#interface f0/5 S1(config-if)# switchport mode trunk S1(config-if)# switchport trunk native vlan 1 S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#interface range f0/1-2, f0/4, f0/6-24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)# switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config)#interface range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configuración de seguridad S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN. S3#config t S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S3(config)#interface f0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1 S3(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)# switchport mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#interface f0/18

	S3(config-if)# switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)# interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración de la seguridad R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#interface g0/1.21 R1(config-subif)# description LAN de Contabilidad R1(config-subif)# encapsulation dot1q 21 R1(config-subif)# ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#interface g0/1.23 R1(config-subif)# description LAN de Ingenieria R1(config-subif)# encapsulation dot1q 23 R1(config-subif)# ip address 192.168.23.1 255.255.255.0

	R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz R1(config)#interface g0/1.99 R1(config-subif)# description LAN de Administracion R1(config-subif)# encapsulation dot1q 99 R1(config-subif)# ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown R1(config-if)#exit

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

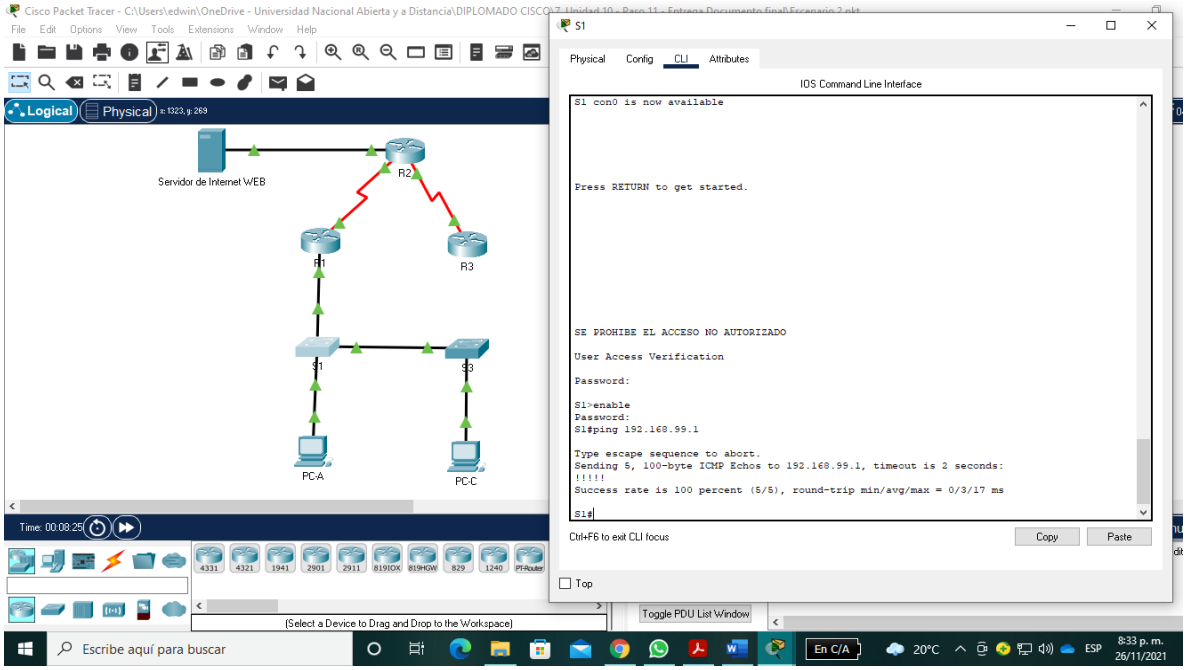
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 17. Verificar la conectividad de red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 99	192.168.99.1	Type escape sequence to abort.

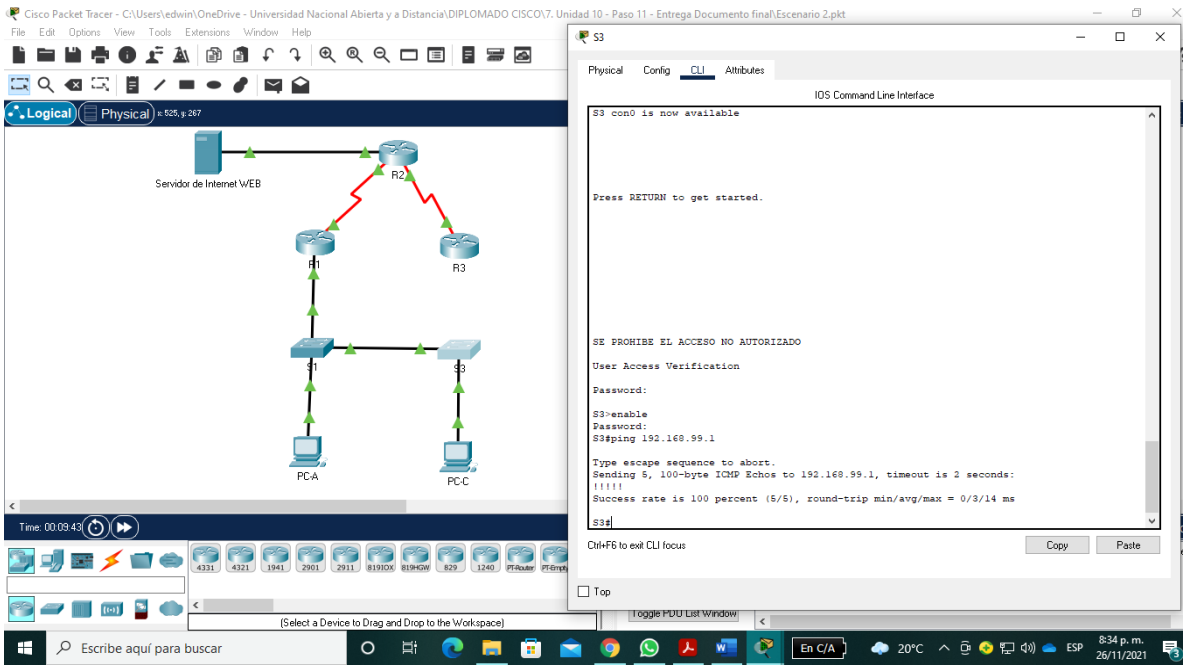
			Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/19 ms
S1	R1, dirección VLAN 21	192.168.21.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

Figura 16. Ping de S1 a R1 VLAN 99



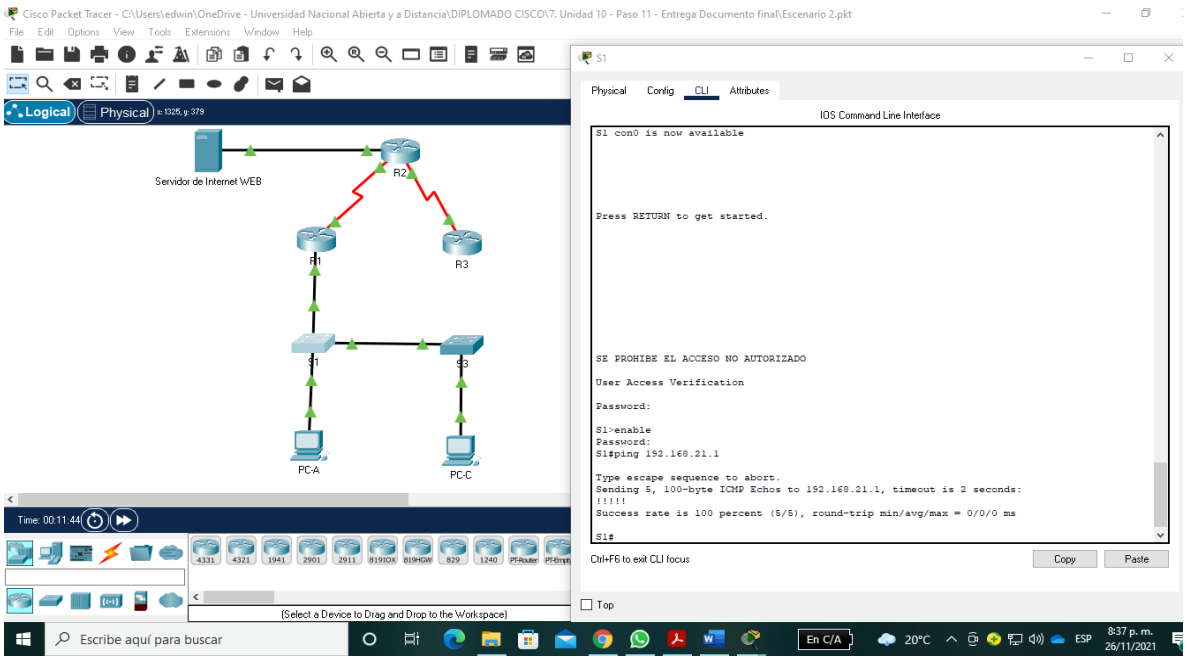
Fuente: Elaboración propia

Figura 17. Ping de S3 a R1 VLAN 99



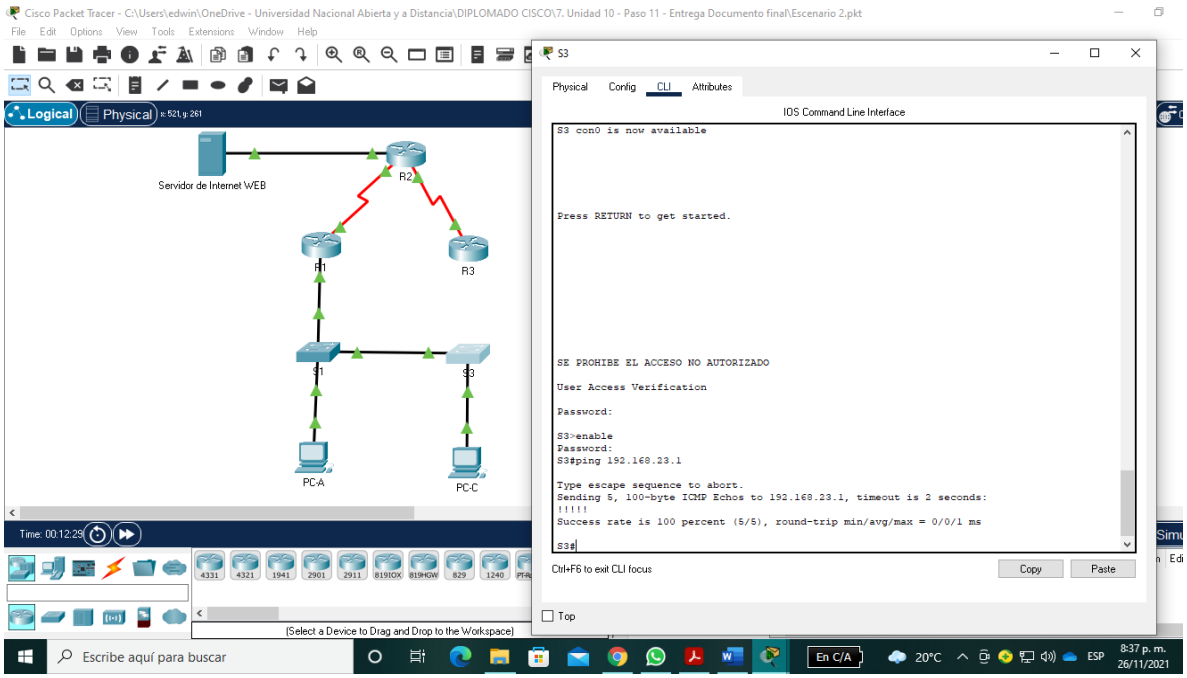
Fuente: Elaboración propia

Figura 18. Ping S1 a R1 VLAN 21



Fuente: Elaboración propia

Figura 19. Ping S3 a R1 VLAN 23



Fuente: Elaboración propia

2.4 Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 18. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)# router ospf 22
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)# network 172.16.1.0 0.0.0.3 area 0 R1(config-router)# network 192.168.21.0 0.0.0.255 area 0 R1(config-router)# network 192.168.23.0 0.0.0.255 area 0 R1(config-router)# network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)# passive-interface g0/1 R1(config-router)# passive-interface g0/1.21 R1(config-router)# passive-interface g0/1.23 R1(config-router)# passive-interface g0/1.99
Desactive la sumarización automática	No se puede hacer en OSPF

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 19. Configuración OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# router ospf 22
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)# network 10.10.10.10 0.0.0.0 area 0 R2(config-router)# network 172.16.1.0 0.0.0.3 area 0 R2(config-router)# network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)# passive-interface loopback0
Desactive la sumarización automática	No se puede hacer para OSPF

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 20. Configuración OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# router ospf 22
Anunciar redes IPv4 conectadas directamente	R2(config-router)# network 172.16.2.0 0.0.0.3 área 0 R2(config-router)# network 192.168.4.0 0.0.0.255 área 0 R2(config-router)# network 192.168.5.0 0.0.0.255 área 0 R2(config-router)# network 192.168.6.0 0.0.0.255 área 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config-router)#passive-interface lo0
Desactive la sumarización automática	No se puede hacer para OSPF

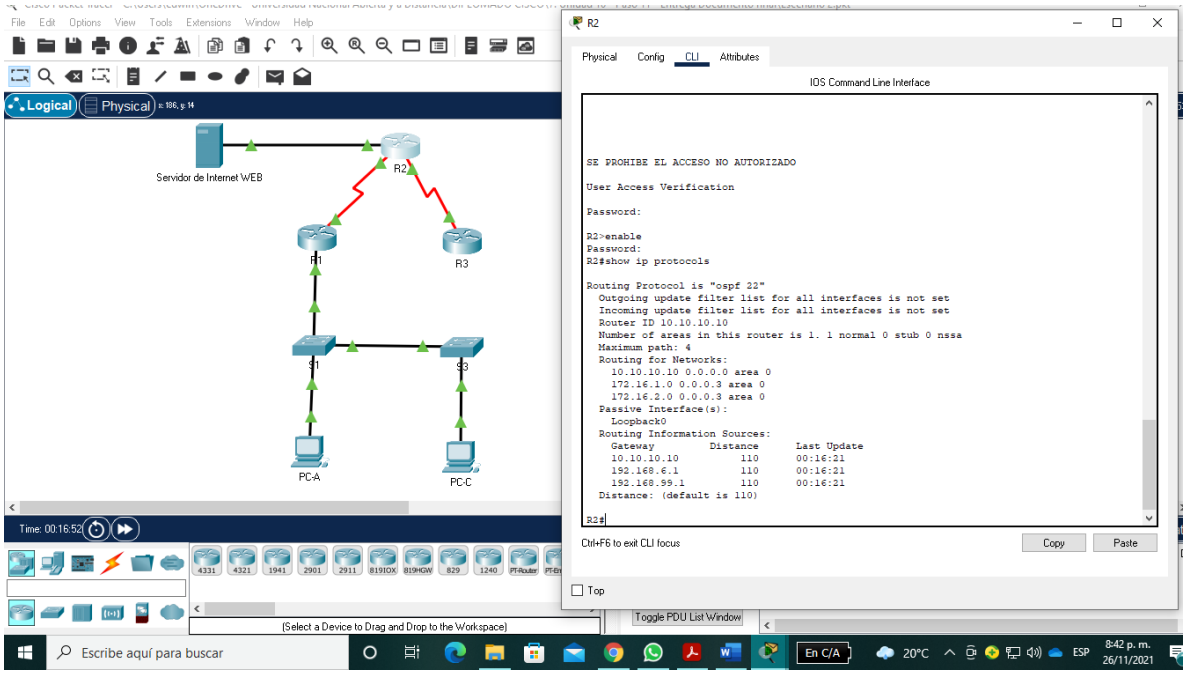
Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 21. Verificación de la información OSPF

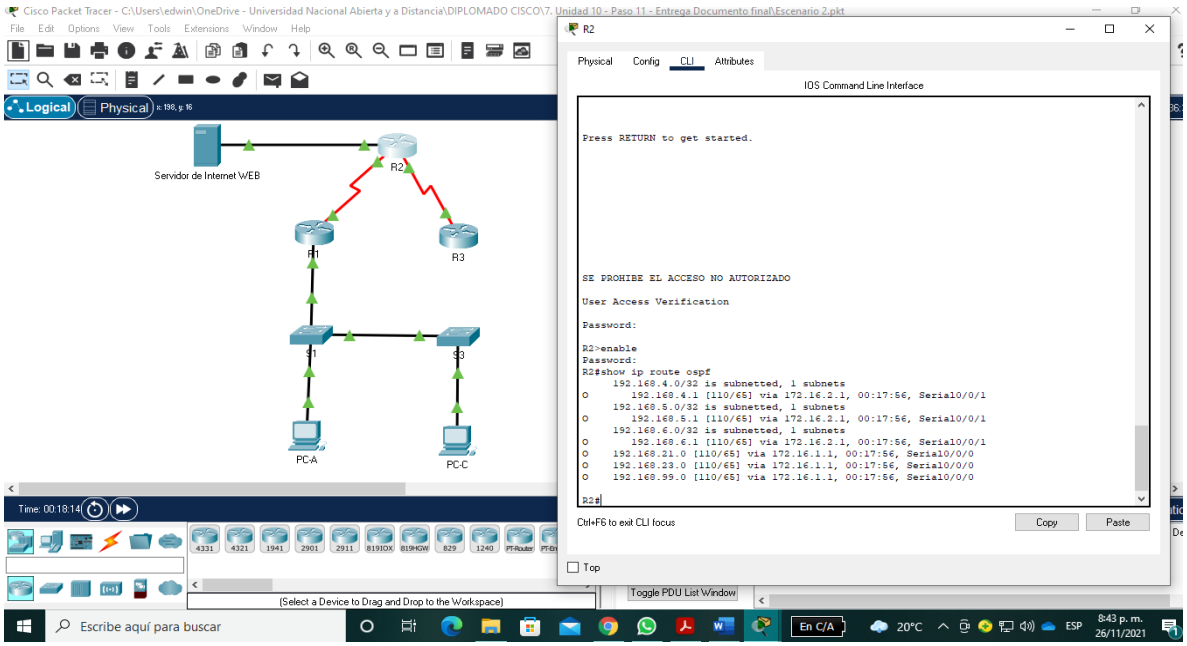
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2# show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2# Show ip route OSPF
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2# Show run

Figura 20. Comando Show ip protocols



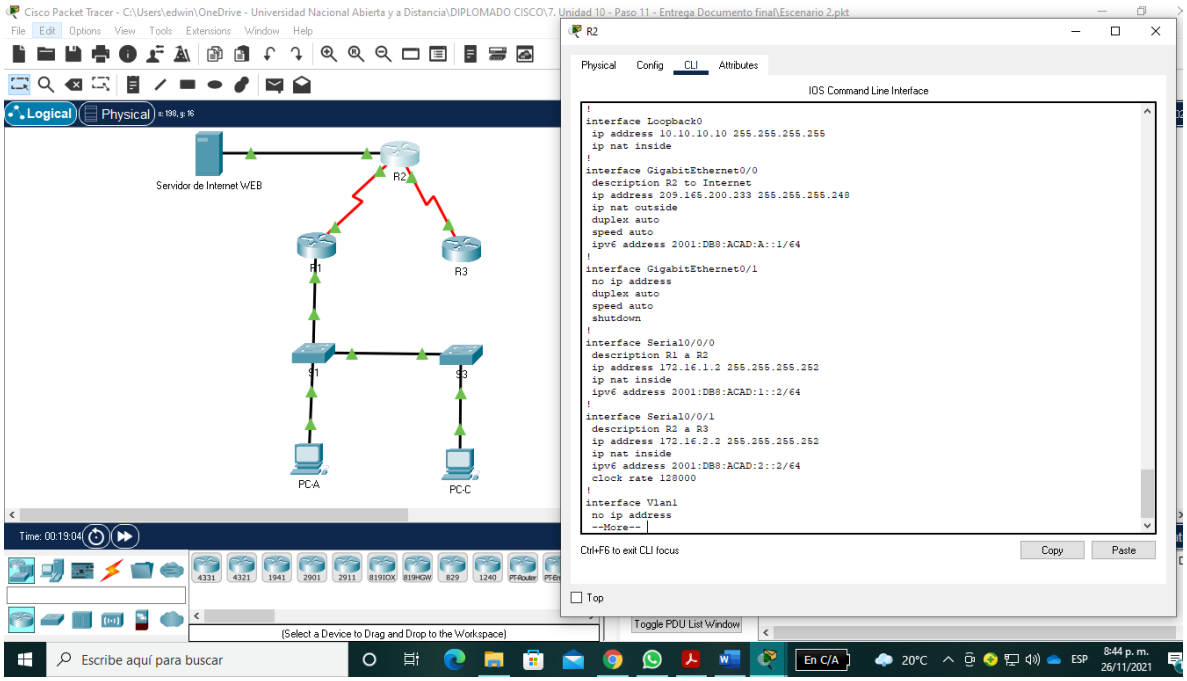
Fuente: Elaboración propia

Figura 21. Comando Show ip route ospf



Fuente: Elaboración propia

Figura 22. Comando show run



Fuente: Elaboración propia

2.5 Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración R1 como servidor DHCP para las vlan 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#(config)ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1#(config)ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com R1#(config)ip dhcp pool ACCT R1#(dhcp-config)#dns-server 10.10.10.10 R1#(dhcp-config)#domain-name ccna-sa.com R1#(dhcp-config)#default-router 192.168.21.1 R1#(dhcp-config)#network 192.168.21.0 255.255.255.0 R1#(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 23. Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#username webuser privilege 15 password cisco12345
Habilitar el servicio del servidor HTTP	No soportado
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No soportado
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Asignar la interfaz interna y externa para la NAT estática	R2(config)# interface g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#int lo0 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0

	0.0.0.255 R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228** R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET. R2(config)#exit

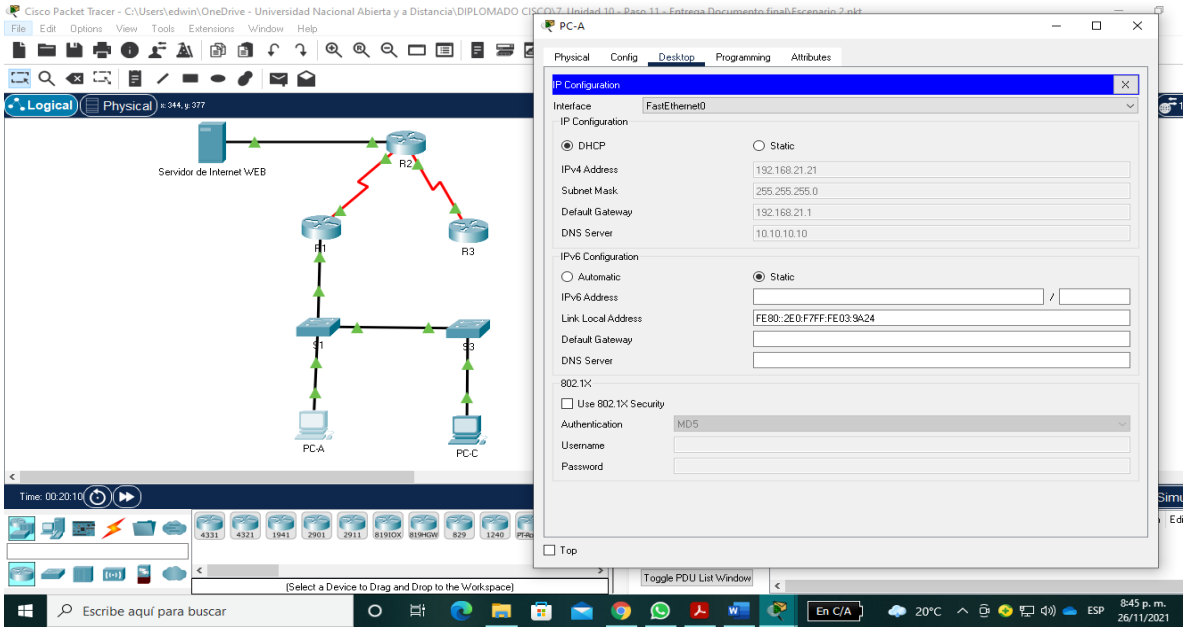
Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pingsse realicen correctamente.

Tabla 24. Verificar el protocolo DHCP y la NAT estática

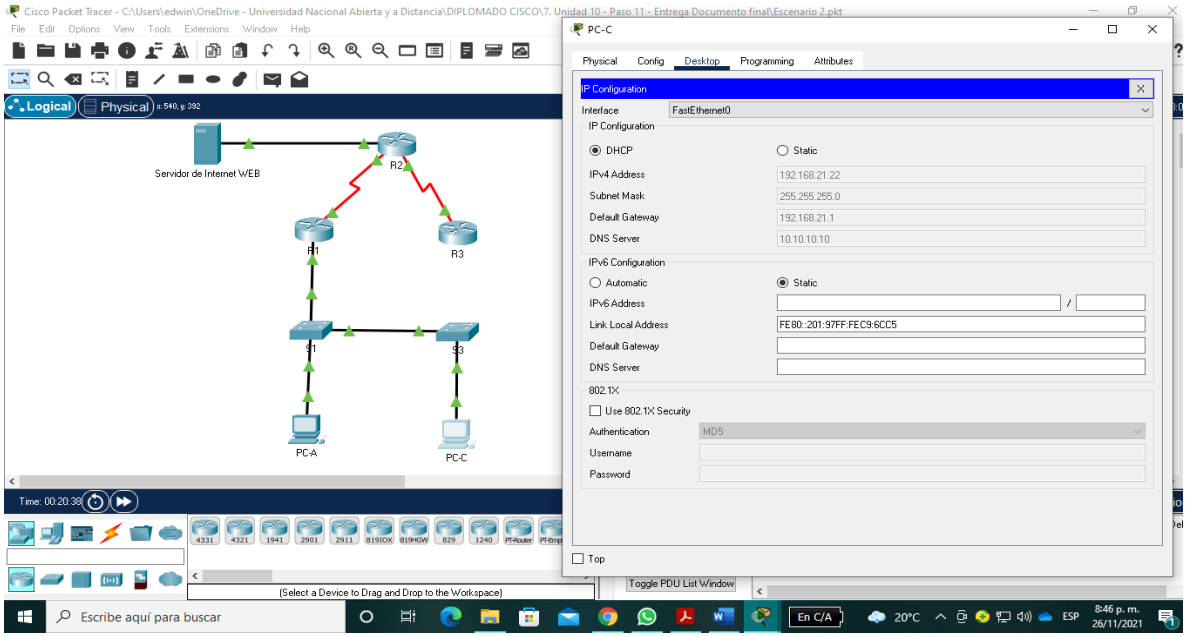
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	El resultado es exitoso para la PC-A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	El resultado es exitoso para la PC-C
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	El resultado es exitoso
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Las PCs, no tienen comunicación a internet al utilizar el comando http server, porque en Packet Tracer es soportado para Activar el servidor web en R2. Por lo tanto, si utilizamos la dirección IP del servidor de Internet en el navegador de la PC-A y PC-C, tendremos acceso a internet.

Figura 23. Verificar que la PC-A haya adquirido información de IP del Servidor DHCP



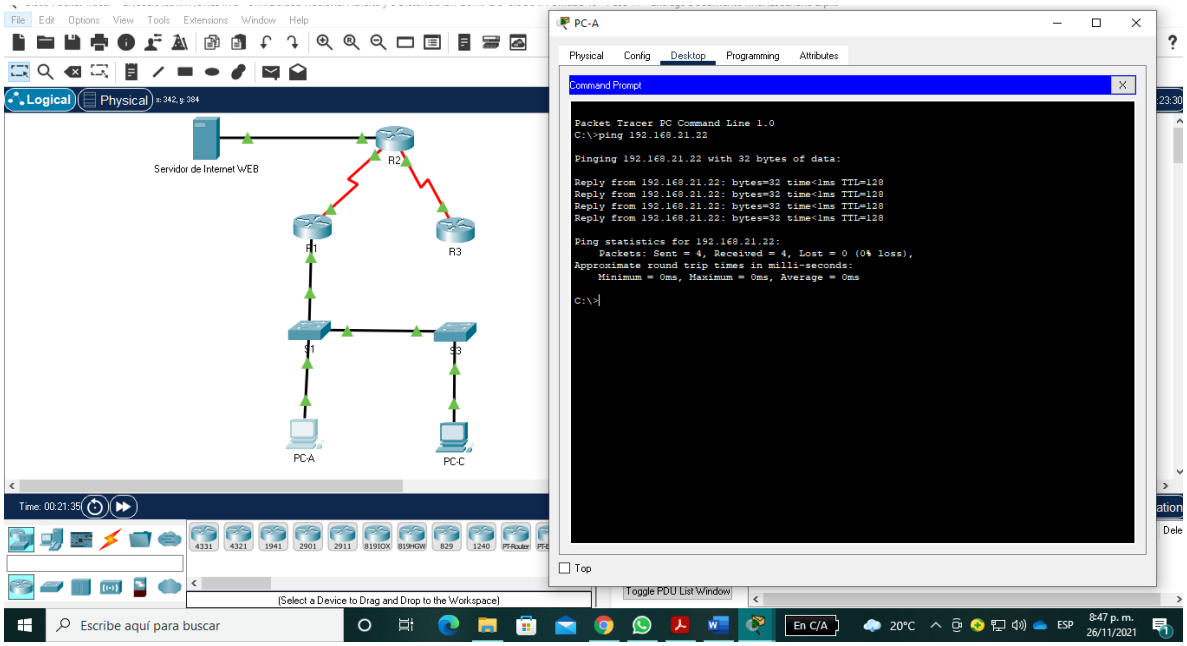
Fuente: Elaboración propia

Figura 24. Verificar que la PC-C haya adquirido información de IP del Servidor DHCP



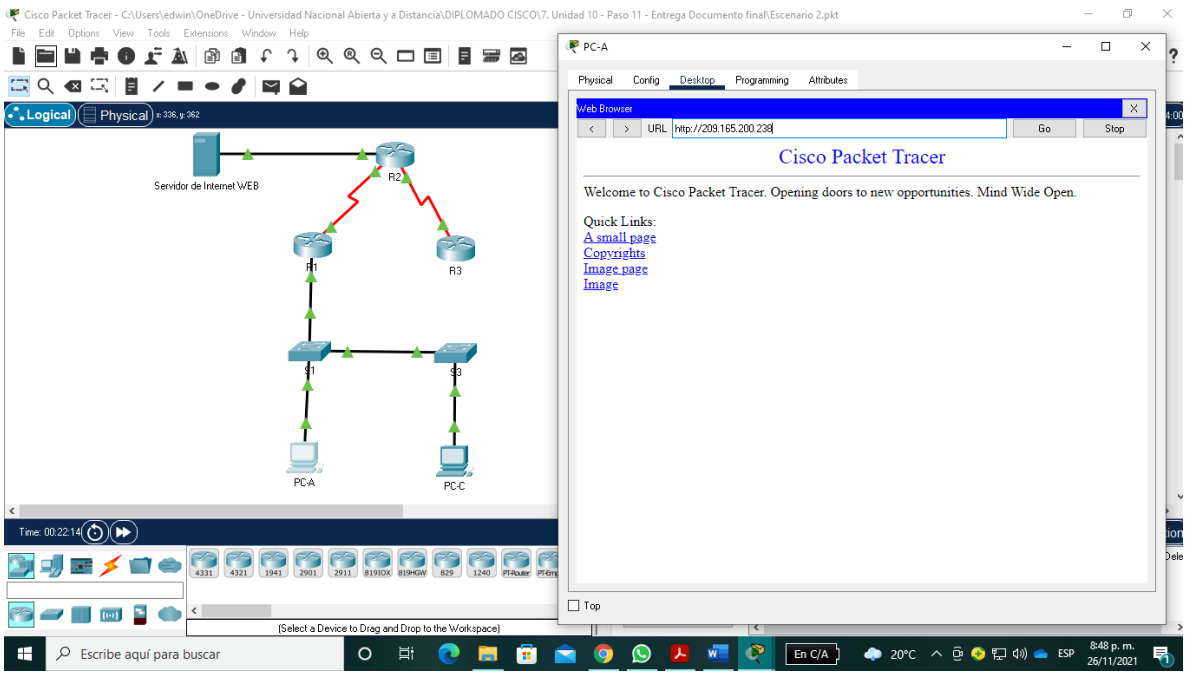
Fuente: Elaboración propia

Figura 25. Verificar que la PC-A pueda hacer ping a la PC-C



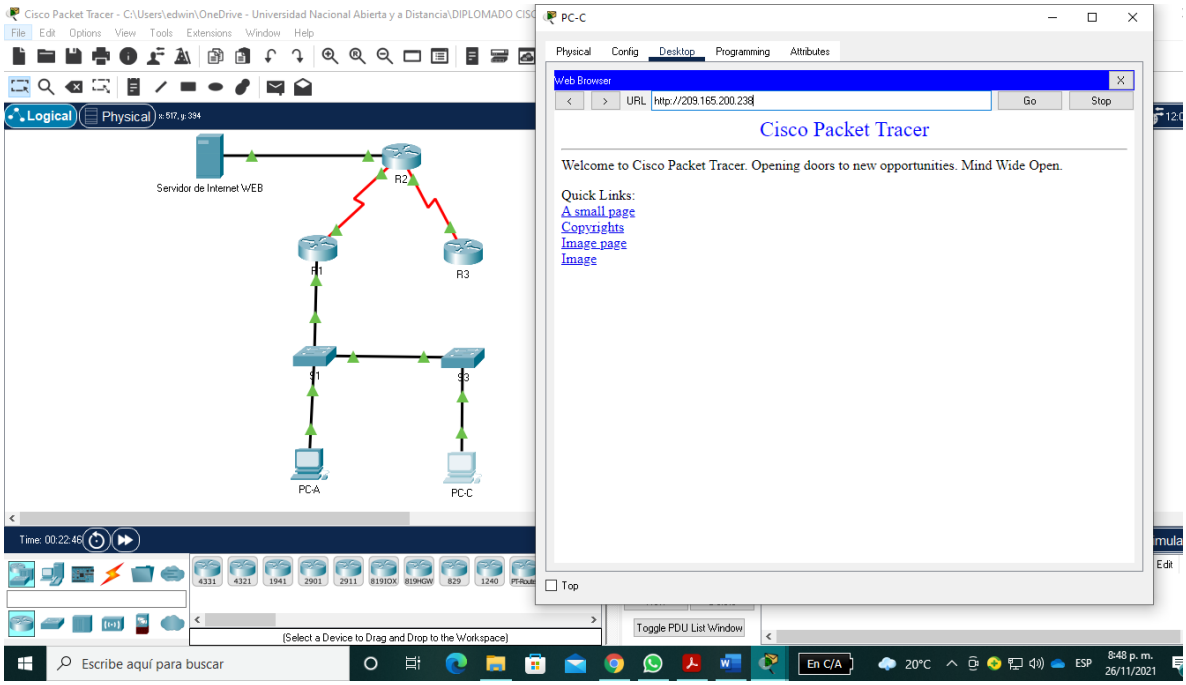
Fuente: Elaboración propia

Figura 26. Conexión a Internet desde PC-A, utilizando la dirección IP del servidor de Internet



Fuente: Elaboración propia

Figura 27. Conexión a Internet desde PC-C, utilizando la dirección IP del servidor de Internet.



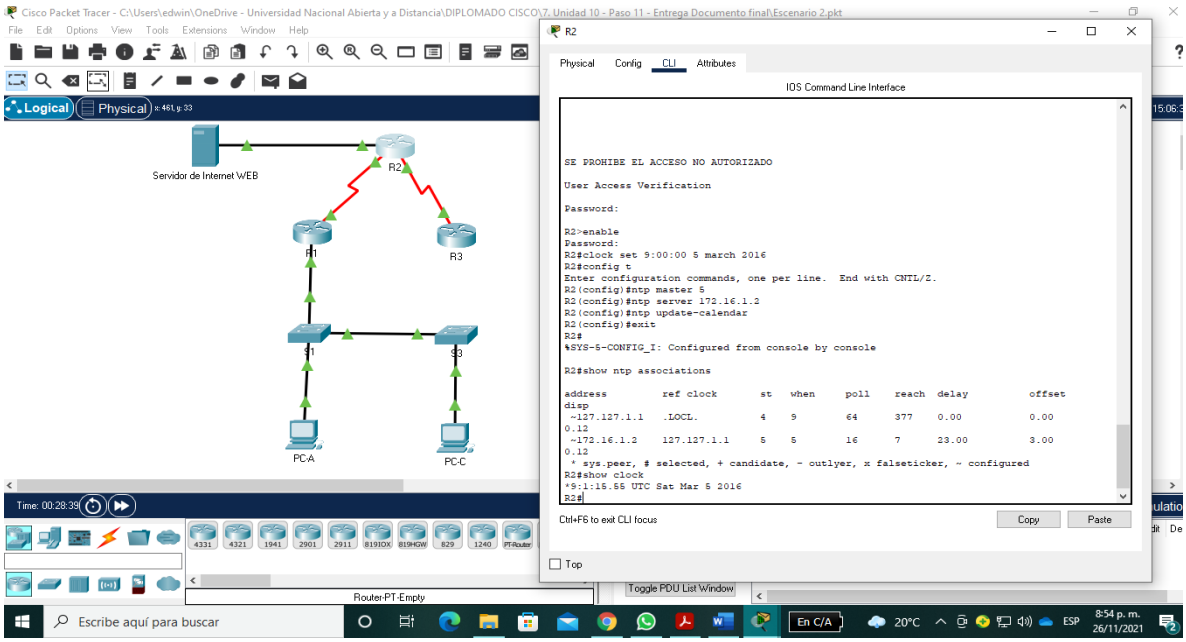
Fuente: Elaboración propia

2.6 Parte 6: Configurar NTP

Tabla 25. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2#config t R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con horaNTP.	R2(config)#ntp update-calendar R2(config)#exit
Verifique la configuración de NTP en R1.	R2#show ntp associations R2#show clock

Figura 28. Verificar la configuración de NTP en R2



Fuente: Elaboración propia

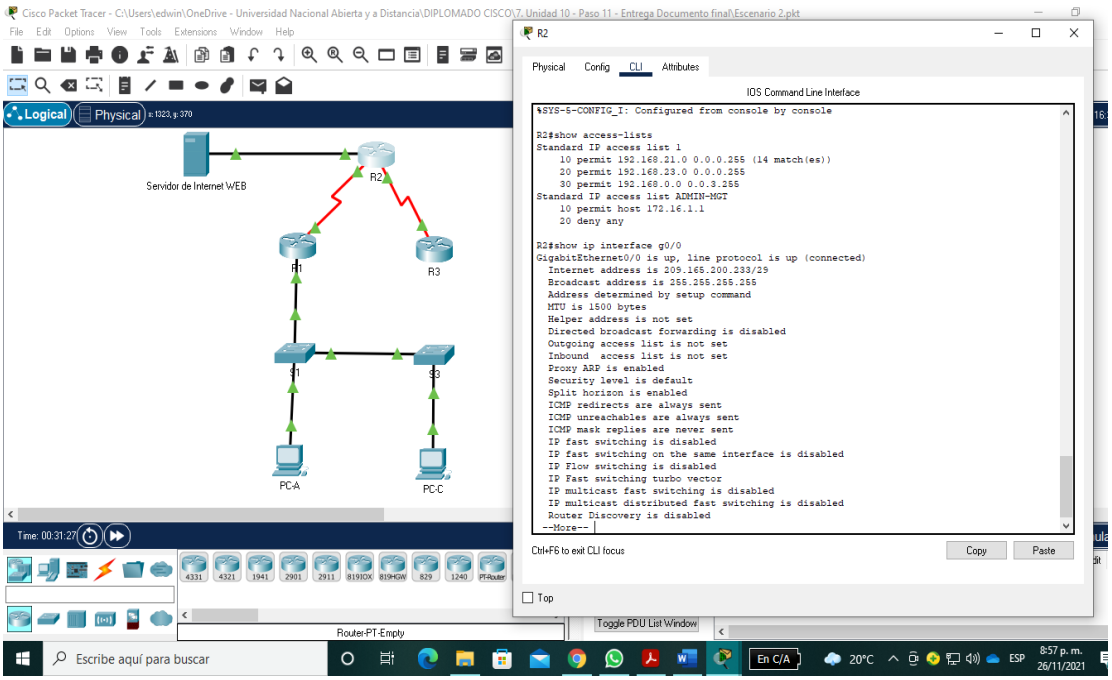
2.7 Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 26. Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R2#config t R2(config)#ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#ip access-class ADMIN-MGT in R2(config-line)#exit
Verificar que la ACL funcione como se espera	R2#Show access-lists R2#show ip interface g0/0

Figura 29. Restringir el acceso a las líneas VTY en Router R2



Fuente: Elaboración propia

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 27. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R1#show ip access-list
Restablecer los contadores de una listade acceso	R1#clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R1#show ip interface
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacerping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-

	A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R1#clear ip nat translation

CONCLUSIONES

De acuerdo con el contenido presentado en los Escenario 1 y 2, se configuraron los dispositivos de la red de acuerdo a los requerimientos dados. La red fue construida con la ayuda del simulador Packet Tracer, donde se diseñaron los respetivos esquemas de direccionamiento IPv4 para la LAN 1 y la LAN 2. Los dispositivos como fueron el Router, el Switch y las dos PCs fueron conectados por medio de cable directo y una vez conectados se procedió a la debida configuración de los mismos.

Los dispositivos como los Routers y el Switches, se configuraron mediante ajustes básicos de seguridad, donde se llevaron a cabo procesos como la creación de usuarios y sus respectivas contraseñas, para ingresar al modo consola de los mismos, dando una plena garantía de seguridad y donde solo podrán acceder los o el usuario que tenga las credenciales y proceder a la configuración que se requiera.

Finalmente, en cada uno de los escenarios propuestos, se documentó debidamente mediante tablas y figuras, el registro de las redes por medio de los comandos comunes de CLI, los cuales muestran y evidencian el debido cumplimento de lo solicitado, y que cumplieron a cabalidad con lo exigido.

BIBLIOGRAFIAS

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11